MODEL SISTEM PENGENDALIAN KEAMANAN KOLABORATIF DALAM DAUR HIDUP PROSES MANAJEMEN KETERSEDIAAN

Rinda Cahyana
Magister Informatika (Sistem Informasi)
Institut Teknologi Bandung

Abstrak - Pengendalian keamanan merupaan bagian terintegrasi dengan manajemen ketersediaan dalam pelaksanaan tata kelola teknologi informasi yang memastikan infrastruktur layanan senantiasa tersedia. Model sistem pengendalian keamanan kolaboratif merupakan gambaran interaksi antara aktor kunci baik manusia maupun mesin yang dipetakan fungsi dan hubungan satu dengan lainnya berdasarkan kerangka kerja *Information Technology Infrastructuire Library*. Pendekatan kolaborasi mengharuskan pengelola layanan teknologi informasi untuk memotivasi pelanggan agar dapat bergabung dalam *Collaborative Work System* secara informal dan berperan aktif dalam menangani hambatan ketersediaan layanan yang dapat menurunkan tingkat kepuasannya dan kepercayaannya terhadap layanan, serta mengatur interaksi sesuai dengan kedudukan dan tanggung jawabnya masing-masing. Keberhasilan penerapan model bergantung kepada kemampuan organisasi dalam menyediakan seluruh komponen *Information Technology Infrastructuire Library* yang terlibat dalam pengendalian keamanan.

Kata Kunci - Tata Kelola, Teknologi Informasi, Manajemen Ketersediaan, *Information Technology Infrastructuire Library*, *Collaborative Work System*, Sistem Interaksi, Keamanan Sistem.

I. PENDAHULUAN

Silang pendapat tentang keutamaan pendekatan sentralistik dan desentralistik dalam pengelolaan Sistem Informasi telah lama terjadi [1,2,3,4]. Sentralisasi menghantarkan kepada spesialisasi, konsistensi, dan kontrol yang lebih terstandarisasi, sedangkan desentralisasi menyediakan kontrol lokal, kepemilikan serta tanggapan dan fleksibilitas dengan kebutuhan bisnis [5,6,7]. Fleksibilitas pada desentralisasi akan menghantarkan kepada standar yang berubah-ubah, sementara sentralisasi akan menyebabkan beban informasi yang berlebihan dan beresiko [8,9]. Pada model tata kelola Teknologi Informasi (TI) federal, keputusan infrastruktur TI adalah sentralistik, sementara keputusan penerapan TI desentralistik [5,7,2,10].

Dalam jurnalnya yang berjudul *"Information Security Control Centralization and IT Governance for Enterprises"*, Robles, Park, dan Kim menyarankan agar pengendalian keamanan dilakukan secara terpusat sehingga kesalahan pengelolaan keamanan desentralistik yang berdampak menyeluruh tidak perlu terjadi [11]. Walau demikian pengendalian keamanan terpusat sebaiknya tidak menghilangkan peran pelanggan sebagai bagian dari *stakeholder*. Penyedia layanan harus memiliki kemampuan integrasi relasional di mana setiap

stakeholder dapat berperan aktif untuk memecahkan masalah sehingga menjadi solusi integratif dan mendefinisikan kemungkinan-kemungkinan di masa mendatang [12]. Henderson menggambarkannya sebagai hubungan strategis yang merefleksikan relasi komitmen jangka panjang, kegunaan kolaborasi mutual, serta resiko dan manfaat bersama [13]. Pelanggan dapat dilibatkan dalam pengelolaan keamanan dengan mengikuti standar penyedia layanan yang memastikan resiko pengelolaannya bersifat lokal atau tidak menyeluruh.

Artikel ini akan merancang dan menerapkan model kolaborasi dalam pengendalian keamanan yang dapat mendorong penyedia dan pengguna layanan berperan aktif dalam mengendalikan keamanan TI, menjadi media interaksi antara penyedia dan pengguna layanann serta alat pemantau, dan sebagai daur hidup proses manajemen ketersediaan yang diharapkan dapat menjaga mutu layanan dan tingkat kenyamanan pelanggan.

II. DASAR TEORI

Tata Kelola Teknologi Informasi

Tata kelola TI adalah penyelarasan strategi TI dengan bisnis seperti dicapainya nilai bisnis secara maksimum melalui pengembangan dan pemeliharaan kendali dan akuntabilitas TI yang efektif, manajemen kinerja, dan manajemen resiko [14]. Tata kelola TI merupakan tanggung jawab eksekutif dan dewan direksi, yang terdiri dari kepemimpinan, struktur organisasi dan proses yang memastikan TI perusahaan mempertahankan dan memperpanjang strategi dan tujuan organisasi [15], yang menspesifikasikan kerangka kerja hak keputusan dan akuntabilitas yang mendorong perilaku yang dikehendaki dalam menggunakan TI [16]. Sejumlah kerangka kerja / *framework* yang mendukung pelaksanaan tata kelola TI telah dibuat. Information Technologi Infrastucture Library (ITIL) memberikan praktik terbaik yang bermanfaat dalam bidang manajemen layanan / *Service Management* dan penyampaian layanan / *Service Delivery*, tetapi tidak menyentuh dampak strategis TI dan hubungannya antara TI dengan Bisnis [17]

Manajemen ketersediaan

Manajemen ketersediaan / *Availability* adalah salah satu dari lima komponen dalam area ITIL *Service Delivery.* Ia bertanggung jawab atas kepastian berjalannya layanan dan senantiasa tersedia untuk dapat digunakan menurut kondisi Perjanjian Mutu Layanan / *Service Level Agreement* (SLA).

Semua area layanan harus dapat diukur dan didefinisikan di dalam SLA. Untuk mengukur ketersediaan layanan area berikut ini biasanya disertakan dalam SLA:

- Statistik perjanjian, seperti apa saja yang termasuk dalam layanan yang disepakati.
- Ketersediaan, seperti kesepakatan waktu layanan, waktu respon, dan lain sebagainya.
- Panggilan *Helpdesk*, seperti jumlah insiden yang diperoleh, waktu respon, waktu resolusi.
- Kontingensi, seperti kesepakatan detail kontingensi, lokasi dokumen, tempat kontingensi, keterlibatan pihak ketiga, dan lain sebagainya.

- Kapasitas, seperti waktu kinerja untuk transaksi online, laporan produksi , jumlah pengguna, dan lain sebagainya.
- Detail pembiayaan, seperti biaya layanan dan setiap hukuman saat layanan tidak terpenuhi.

Ketersediaan biasanya dihitung berdasarkan model yang melibatkan rasio ketersediaan dan teknik seperti *Fault Tree Analysis*, dan meliputi elemen berikut ini:

- *Serviceability*, yakni tatkala layanan diberikan oleh organisasi pihak ketiga, ini adalah komponen ketersediaan yang diharapkan.
- *Reliability*, yakni waktu untuk komponen dapat dilaksanakan dalam kondisi spesifik tanpa kegagalan.
- *Recoverability*, yakni waktu yang harus digunakan untuk mengembalikan kondisi komponen seperti sedia kala.
- *Maintainability*, yakni pemeliharaan komponen apakah karena perbaikan ataupun untuk pencegahan.
- *Resilience*, yakni kemampuan untuk menghadapi kegagalan,
- *Security*, yakni kemampuan komponen dalam menangani pelanggaran keamanan.

Aktivitas manajemen ketersediaan meliputi:

- Memastikan ketersediaan layanan memenuhi SLA
- Menentukan penyebab kegagalan dalam penyediaan layanan
- Meninjau ketersediaan bagi kebutuhan bisnis dari system bisnis
- Mencatat kebutuhan bisnis
- Memastikan rencana kontingensi yang tepat tersedia dan telah diuji

Keamanan TI adalah bagian yang terintegrasi dengan manajemen ketersediaan, dan menjadi focus primer yang memastikan infrastruktur TI terus tersedia untuk layanan TI. Analisis resiko merekomendasikan kendali untuk meningkatkan ketersediaan infrastruktur TI, seperti standar pengembangan, pengujian, pengamanan fisik, kemampuan yang tepat, dan lain sebagainya.

Sistem Kerja Kolaborasi

Kolaborasi adalah kerja kolektif dua tau lebih orang atau organisasi yang bekerja sama untuk mencapai tujuan bersama dengan cara berbagi pengetahuan, belajar dan membangun konsensus. Kebanyakan kolaborasi memerlukan kepemimpinan, meskipun bentuk kepemimpinannya dapat sosial dalam desentralisasi dan kelompok egaliter [18]. Agar kolaborasi berhasil, diperlukan kejelasan peran dan tanggung jawab dari setiap individu dan panduan untuk mencapai tujuan kolektif. Peran setiap individu dalam tata kelola TI dijelaskan melalui deskripsi kerja dan SLA, sementara panduan untuk mencapai tujuan kolektif adalah melalui kebijakan dan prosedur.

Sistem kerja kolaboratif / *Collaborative Work System* (CWS) adalah unit organisasi yang terjadi pada saat kolaborasi berlangsung, baik secara formal maupun informal, dan dilakukan secara sengaja atau tidak. Jenis CWS antara lain sebagai berikut:

1. Level Kelompok

a. Tim, yakni kelompok orang yang memiliki pekerjaan yang saling berkaitan dan berbagi tujuan dan mengadakan tanggung jawab untuk tujuan bersama.
b. Komunitas praktis, yakni kelompok informal atau jaringan orang yang berbagi ketertarikan, cerita, dan bahasa umum, tetapi lepas tanggung jawab.

2. Level Organisasi
   a. Organisasi berbasis tim, yakni unit kerja, manajer di dalam team, dan organisasi dirancang untuk mendukung tim.
   b. Organisasi kolaboratif, yakni tim yang digunakan jika diperlukan, mendukung kolaborasi formal maupun informal, dan organisasi dirancang untuk mendukung kolaborasi.

Alasan fokus terhadap CWS:

- Untuk menciptakan keuntungan kompetitif. Organisasi yang bekerja kolaboratif dan melakukannya dengan baik, akan sukses dalam lingkungan sekarang ini.
- Untuk menciptakan konteks bagi kesuksesan tim. Tim dan struktur kolaboratif lainnya memiliki kesempatan sukses yang jauh lebih baik jika organisasi dirancang untuk mendukung kolaborasi.
- Untuk mempromosikan integrasi dan keselarasan lateral. Memfokuskan diri terhadap CWS artinya tidak hanya meningkatkan kolaborasi di dalam kelompok, tetapi di antara kelompok. Integrasi lateral ini mempromosikan kinerja signifikan di antara tim dan mengurangi kegagalan tim yang terisolir.
- Penghubung terbaik bagi lingkungan. Menciptakan kesadaran akan kebutuhan untuk bertahan dan berkembang.
- Meningkatkan fleksibilitas. Kemampuan kolaborasi memberikan fleksibilitas untuk memenuhi kebutuhan lingkungan (termasuk pelanggan), yang meningkatkan keberhasilan jangka panjang organisasi.

Dengan demikian CWS dapat meningkatkan kinerja, menciptakan keuntungan berbasis kepentingan yang kompetitif dan memenuhi kebutuhan individual maupun kolektif, membangun budaya kolaborasi dalam lingkungan TI yang berubah untuk berbagi kekuatan dalam mempertahankan dan mengembangkan kebutuhan dan layanan, serta menjadikan resiko TI sebagai tanggung jawab bersama agar layanan tetap tersedia.

III. ANALISIS PERMASALAHAN

Kebutuhan Model Kolaborasi Dalam Pengendalian Keamanan

Dalam studi kasus Robles, Park, dan Kim dibandingkan dua pendekatan pengendalian keamanan dari dua jenis tata kelola keamanan TI, yakni sentralistik di mana pengendalian keamanan dilakukan secara terpusat, dan desentrasitik di mana pengendalian keamanan dapat dilakukan oleh setiap pengguna termasuk tanggung jawab keamanan terkait dengan aktivitasnya. Dalam kasus penanganan *malware*, model kendali keamanan terpusat berhasil menangani *malware* secara keseluruhan. Sementara dalam model kendali keamanan desentralistik, penanganan *malware* bergantung kepada tingkat kesadaran dan penguasaan

teknologi dari *end user*. Apabila tingkatnya rendah, maka *malware* tidak tertangani dan keberadaannya dapat mengancam pengguna lainnya [11].

Dalam kesimpulannya disebutkan bahwa keamanan harus dikelola secara terpusat dan peran aktif pengguna yang selama ini berlaku dalam pendekatan desentralisasi seperti pemeriksaan dan deteksi penyusupan tetap dipertahankan [11]. Kesimpulan tersebut mengindikasikan bahwa harus ada model kolaborasi antara manajemen ketersediaan dan pelanggan yang diterapkan secara baik, dengan peran dan tanggung jawab yang jelas dan proporsional, sehingga tujuan keamanan bersama tercapai. Namun dalam jurnal tersebut tidak digambarkan bagaimana model kolaborasi *end-user* dan penyedia layanan TI menurut kerangka kerja yang mendukung tata kelola TI, khususnya kerangka kerja ITIL.

Manajemen Ketersediaan dan Model Sistem Pengendalian Keamanan Kolaboratif

Keamanan merupakan persoalan bersama yang menggangu layanan dan dapat menurunkan kenyamanan pelanggan. Ancaman keamanan dapat bersumber dari pelanggan atau dari pihak penyedia layanan. Dengan sumber dari dua arah tersebut maka diperlukan komunikasi dan kerja sama di antara penyedia layanan dan pelanggan sehingga ancaman terhadap ketersediaan layanan diketahui sesegera mungkin, dan penangannya dapat dilakukan sesegera mungkin baik oleh penyedia layanan melalui dukungan teknisnya ataupun oleh pelanggan sendiri yang dipandu oleh *helpdesk.*

Dalam menangani masalah, semua pihak yang terlibat dalam penanganan masalah bekerja sama membentuk CWS baik secara formal maupun tidak untuk mencapai tujuan bersama, yakni menghilangkan hambatan ketersediaan layanan, dengan saling berbagi informasi seputar penyebab masalah, dan melakukan upaya penanganan terintegrasi berdasarkan kebijakan dan prosedur yang ditetapkan penyedia layanan.

Sebagai komponen yang bertangggung jawab atas pengendalian keamanan, manajemen ketersediaan adalah pihak yang harus memahami secara benar bagaimana kolaborasi dibangun dengan pelanggan. Manajemen ketersediaan merupakan pemimpin yang harus dapat mengendalikan setiap orang yang terlibat dalam usaha bersama menangani hambatan ketersediaan layanan agar melaksanakan peran sesuai dengan tanggung jawabnya, sehingga segala tindakan yang diambil oleh setiap orang merupakan tindakan integratif, terkendali, dan sesuai dengan kebijakan dan prosedur, sehingga hasilnya dapat memenuhi SLA. Manajemen ketersediaan harus dapat mendorong dan menyadarkan para pengguna akan arti penting kesertaan mereka dalam mengawasi dan mengendalikan keamanan layanan demi kenyamanan mereka dan pemenuhan SLA oleh penyedia layanan.

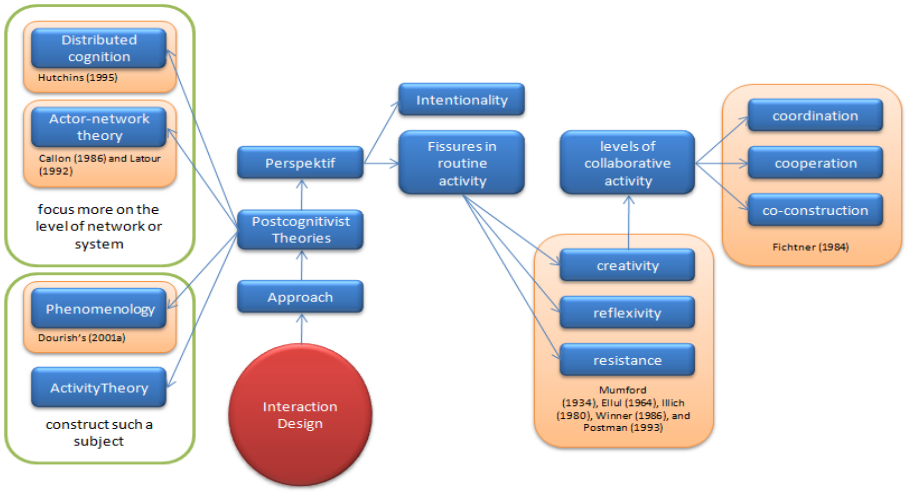
Sementara itu, pelanggan atau pengguna yang berpartisipasi dalam pengendalian keamanan, adalah mereka yang sadar dan termotivasi. Tugas mereka adalah melaporkan segala gangguan yang terjadi sebelum atau setelah interaksi mereka dengan perangkat teknologi. Apapun yang dianggap menggangu kenyamanan mereka harus segera dilaporkan kepada penyedia layanan melalui *Service Desk* atau *Help Desk*, sehingga gangguan tersebut dapat segera ditindak lanjuti dan diselesaikan oleh penyedia layanan untuk memenuhi SLA.

Namun ada kalanya pelanggan tidak menyampaikan masalahnya kepada penyedia layanan dan malah membuat keresahan bagi pelanggan lainnya melalu forum, yang pada akhirnya menurunkan tingkat kepercayaan pelanggan kepada penyedia layanan. Kondisi seperti ini dapat disebabkan karena ketidaktahuan pelanggan akan ketersediaan *Service Desk* yang senantiasa siap membantu semua persoalan yang dihadapinya, atau karena akumulasi kekesalan karena tingginya frequensi gangguan atau kegagalan dalam memenuhi SLA, atau karena penyedia layanan tidak menyelenggarakan *Service Desk* secara baik.

Dalam ketertutupan komunikasi seperti ini, satu-satunya harapan penyedia layanan untuk mengetahui masalah adalah perangkat pengawasan infrastruktur TI. Melalui perangkat ini, diharapkan dapat diketahui hambatan layanan dan ditangani secara cepat oleh dukungan teknis. Sebagai sumber informasi kedua, perangkat ini memiliki peran yang sama dan menjadi entitas penting dalam CWS.

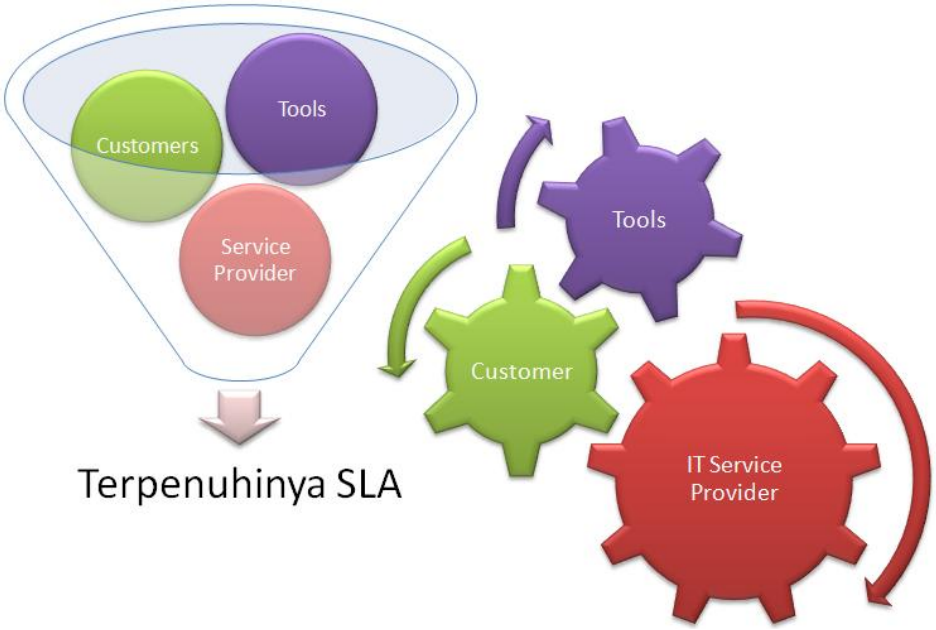
Penggalian Aktor dengan Pendekatan Postcognitivist Theories

Dalam CWS terjadi berbagai bentuk interaksi. Pendekatan *Postcognitivist Theories* dalam pengembangan sistem interaksi dapat digunakan untuk memastikan siapa saja yang boleh dan harus terlibat dalam kolaborasi, sehingga kunci sukses pengendalian keamanan dapat diidentifikasi. Kaptelinin dan Nardi berpendapat bahwa teori tersebut penting bagi perancangan interaksi. Keduanya mengamati bahwa pengembangan beragam teori memberi kesempatan untuk setiap teori saling menyempurnakan dan mengkontribusikan sekumpulan perspektif dan konsep unik [19].



Gambar 1. *Mindmap* Perancangan interaksi dengan pendekatan *Postcognitivist Theories*.

Dengan menggunakan pendekatan *actor-network theory* [20] dan *distributed cognition* yang menempatkan manusia dan bukan manusia sebagai media atau aktor yang sama dalam sistem [21], maka pengendalian keamanan merupakan hasil kolaborasi dari tiga aktor berikut ini:



Gambar 2. Pengendalian Keamanan Kolaboratif

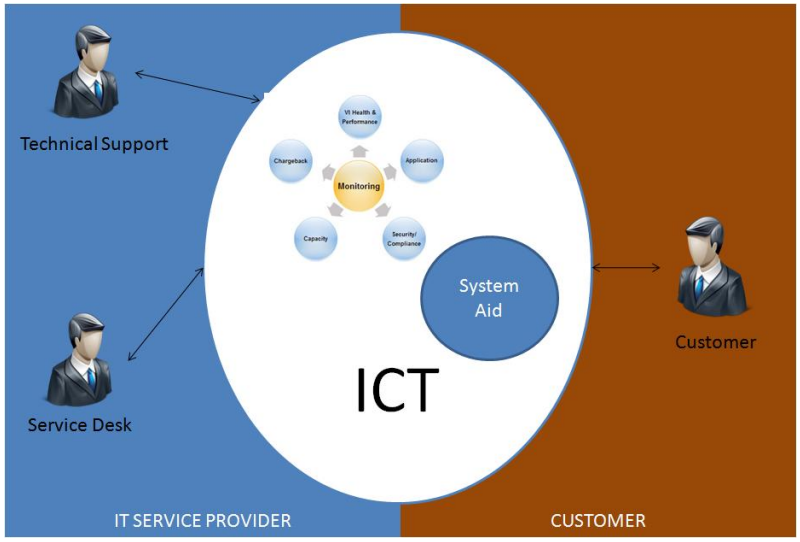
Sebelah kanan menunjukan kesamaan peran dan kepentingan antara ketiga aktor dan menjadikan pemenuhan SLA yang dibangun di antara pelanggan dan penyedian layanan sebagai tujuan bersama. Sementara bagian kiri menunjukan tanggung jawab besar penyedia layanan TI dalam mengendalikan keamanan di bandingkan pelanggan sekalipun terpenuhinya SLA adalah kepentingan pelanggan.

Setelah aktor yang berinteraksi dalam CSW diketahui, permasalahannya adalah bagaimana memetakan aktor tersebut ke dalam model pengendalian keamanan kolaboratif menurut kerangka kerja ITIL.

IV. DESAIN MODEL KOLABORASI

Model Kolaborasi Level Konteks

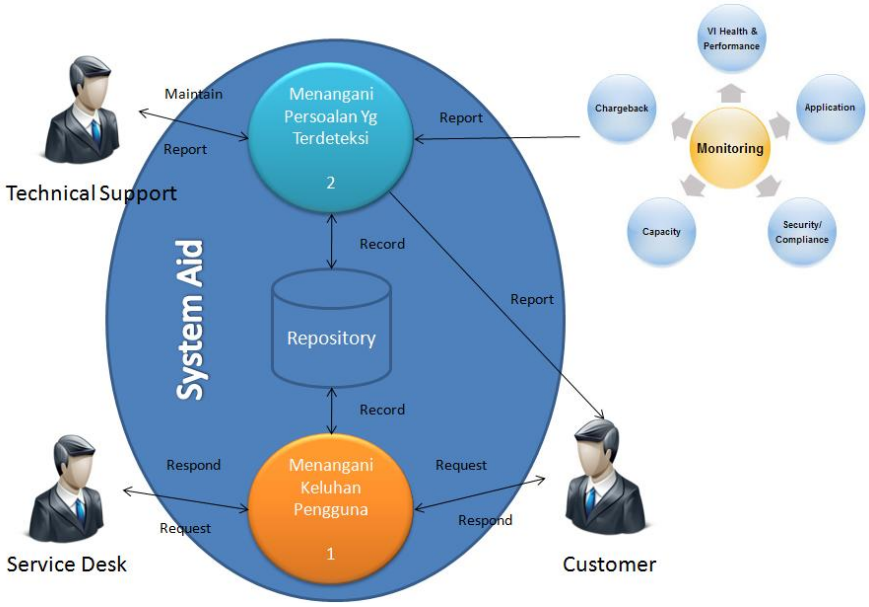
Dalam level konteks sebagaimana tampak pada gambar 3 terlihat bahwa terdapat tiga entitas utama dalam pengendalian keamanan yakni *Service Desk* yang berhadapan langsung dengan *End-User* dan *Technical Support* yang memberi dukungan terhadap layanan TI dan didukung oleh perangkat pengawasan. Sementara informasi antara Service Desk dengan Technical Support dilakukan melalui *System Aid*. Dalam menangani masalah keamanan ketiganya harus bekerja sama sebagai sebuah tim yang saling berkomunikasi melalui *Information and Communication Technology* (ICT) dalam proses identifikasi penyebab hambatan ketersediaan layanan yang sedang dihadapi. Kesertaan *End-User* dalam tim merupakan kesertaan informal, karena ia tidak diberi tanggung jawab besar dalam menangani persoalan. Sementara dua entitas lainnya yang merupakan bagian dari penyedia layanan merupakan anggota tim formal karena keduanya memiliki tanggung jawab untuk menangani persoalan keamanan dan memenuhi SLA.



Gambar 3. Model Sistem Pengendalian Keamanan Kolaboratif Level Konteks

Model Kolaborasi Level 1

Level 1 menunjukan dua proses utama dalam pengendalian keamanan yakni 1) Menangani Keluhan Pengguna sebagai proses komunikasi dan kolaborasi antara pelanggan dengan *Service Desk*, dan 2) Menangani Persoalan Yang Teridentifikasi sebagai proses komunikasi dan kolaborasi antara *Technical Support*, pelanggan, dan perangkat pengawasan.

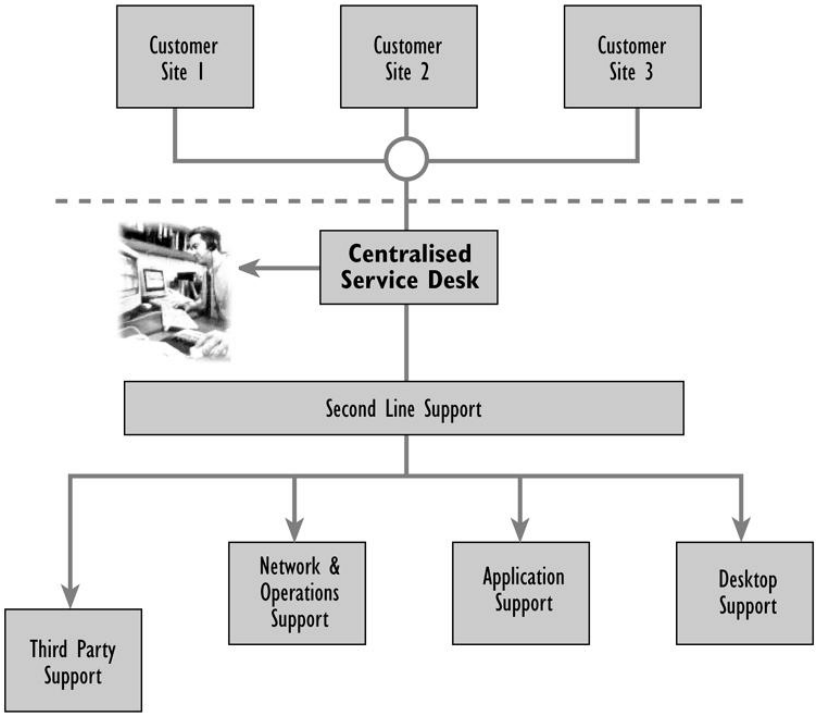


Gambar 4. Model Sistem Pengendalian Keamanan Kolaboratif Level 1

Kolaborasi di antara empat entitas terjadi melalui ICT dan informasi dalam konteks penananganan masalah disalurkan melalui *Configuration Management Database* (CMDB), yakni gudang (*repository*) informasi terkait seluruh komponen system informasi. Dalam konteks ITIL, CMDB merepresentasikan kewenangan konfigurasi atas komponen penting dalam lingkungan TI. CMDB membantu organisasi memahami hubungan antara semua komponen dan menelusuri konfigurasinya. CMDB merupakan komponen mendasar dari proses Manajemen Konfigurasi kerangka kerja ITIL.

CMDB merekam (*record*) item konfigurasi / *Configuration Items* (CI) dan detail tentang atribut penting dan hubungan di antara CI. Manager konfigurasi biasanya menjelaskan CI menggunakan atribut konfigurasi: Teknis, Kepemilikan, dan Hubungan. Kunci sukses dalam menerapkan CMDB adalah kemampuan dalam menemukan informasi tentang CI secara otomatis (*auto-discovery*) dan menelusuri perubahan yang terjadi padanya.

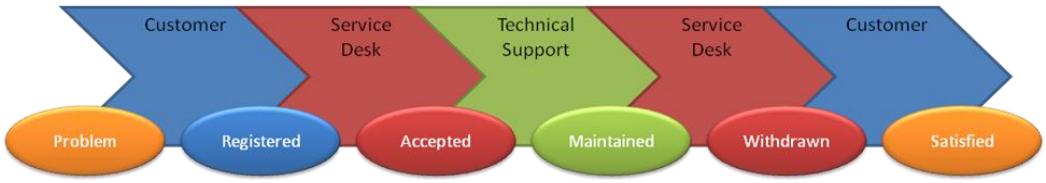
Dalam proses 1, pengguna dapat berpartisipasi dalam CSW secara tidak formal dengan melakukan pengawasan terhadap infrastruktur TI melalui panel kontrol nya dan melaporkan ganguan keamanan kepada *Service Desk*. Misalnya pengguna mengetahui adanya serangan virus setelah perangkat Symantec Anti Virus Server yang melakukan pemindaian terjadwal terhadap semua computer klien menginformasikan keberadaan virus pada computer klien yang terinfeksi, atau setelah pengguna melakukan pemeriksaan sendiri.



Gambar 5. *Service Desk* Terpusat [17]

Troubleshooting untuk ganguan keamanan tersebut dicari penyelesaiannya oleh *Service Desk* melalui gudang pengetahuan / *Knowladge Repository* (KR) yang terdapat dalam *System Aid*. Jika *troubleshooting* nya ditemukan maka *Service Desk* akan merespon laporan pelanggan dengan memandu sehingga pelanggan dapat melakukan *troubleshooting* sendiri. Apabila pelanggan tidak berhasil melakukan *troubleshooting* sendiri atau apabila pengetahuan yang diperlukan tidak ada, *Service Desk* akan mengkonfirmasi masalah ganguan ketersediaan layanan tersebut melalui *System Aid* kepada *Technical Support* untuk ditangani. *Technical Support* yang dihubungi sesuai dengan masalah yang dihadapi, apakah *Third Party Support*, *Network & Operations Support*, *Application Support*, atau *Desktop Support*. Masalah baru yang belum tersedia pengetahuannya kemudian ditambahkan oleh *Technical Support* ke dalam KR.

Dalam proses 2, *Technical Support* bersikap reaktif menangani masalah begitu permasalahan teridentifikasi baik melalui KR maupun perangkat pengawasan. *Technical Support* memperbaharui informasi CI terkait sehingga *Service Desk* dapat menginformasikan permasalahnya kepada pelanggan dan mencatat langkah penanganannya dalam KR dan menetapkannya sebagai prosedur standar penanganan masalah tersebut.



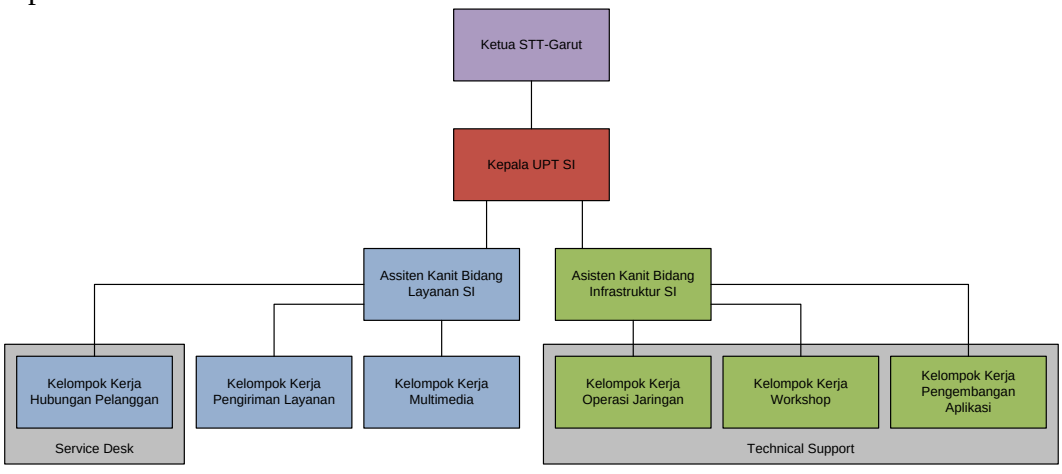
Gambar 6. Daur hidup pemeliharaan infrastruktur TI [17]

Gambar 6 menunjukan proses pemeliharaan infrastruktur yang dilakukan oleh *Technical Support* terkait penanganan masalah keamanan yang diajukan oleh pelanggan yang tidak dapat ditangani oleh *Service Desk*. Proses dimulai dari permasalahan yang dialami oleh pelanggan yang menyebabkannya mendaftarkan masalah tersebut untuk ditanggapi oleh *Service Desk* melalui infrastruktur ICT. Setelah masalah diketahui oleh *Service Desk* dan dan tidak dapat memberikan solusi, *Service Desk* kemudian menyampaikan masalah tersebut kepada *Technical Support* terkait. Proses selanjutnya adalah dilakukannya pemeliharaan terhadap infrastruktur ICT yang bermasalah oleh *Technical Support* dengan memenuhi SLA. Setelah selesai, *Technical Support* memperbaharui CMDB dan masalahpun ditutup. Setelah masalah tersebut diselesaikan, pelanggan merasa puas.

V. IMPLEMENTASI DAN HASIL

Restrukturisasi Organisasi

Implementasi model kolaborasi tersebut dilakukan di UPT Sistem Informasi (USI) Sekolah Tinggi Teknologi Garut. Untuk menerapkan model ini, terlebih dahulu USI mengembangkan organisasi sesuai dengan ketersediaan layanan dan kebutuhan model. Struktur organisasinya kemudian dikembangkan menjadi seperti ini:



Gambar 8. Struktur Organisasi USI STT-Garut

Gambaran umum peran atau tanggung jawabnya adalah sebagai berikut:

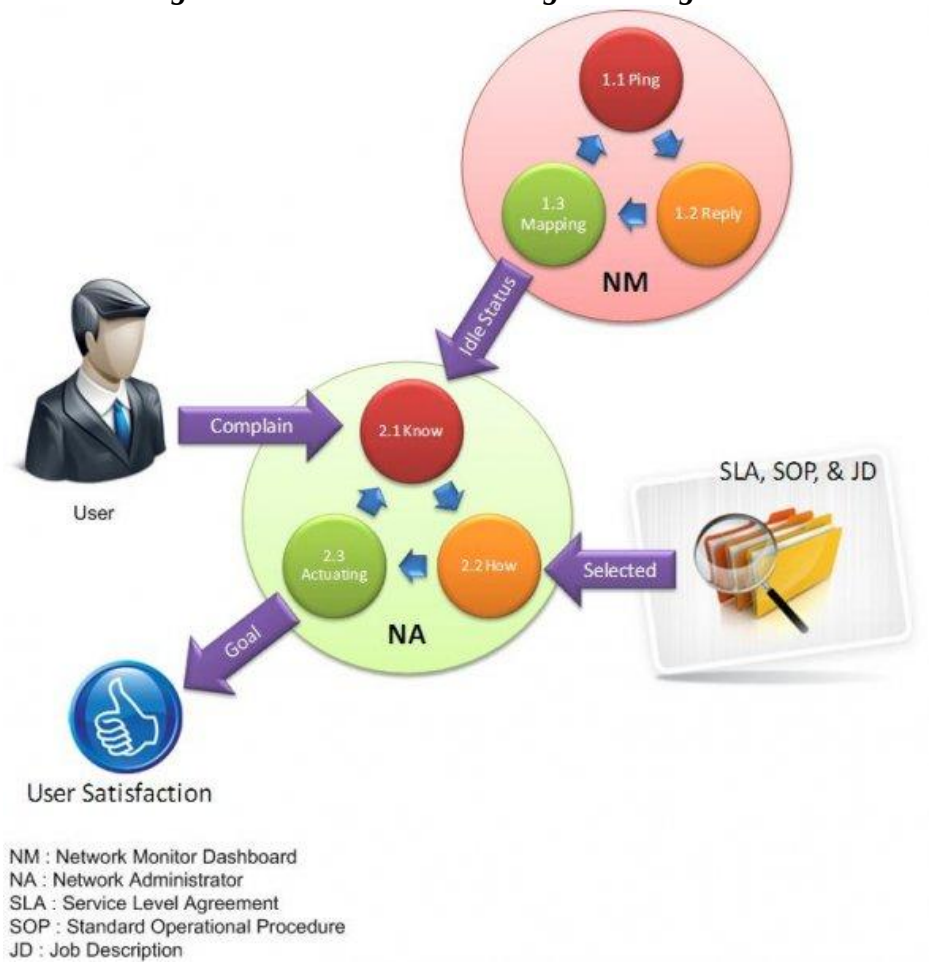
- Layanan SI diselenggarakan USI sesuai dengan kebutuhan pengembangan SI yang ditetapkan oleh ketua STT-Garut melalui Rencana Strategis (Renstra) STT-Garut.
- Kepala USI menerjemahkan kebutuhan tersebut dalam Rencana Induk Pengembangan Sistem Informasi.
- Operasional harian layanan SI dalam area Layanan dan Infrasruktur dikordinasikan oleh Asisten kepala USI. Kedua Asisten tersebut bertanggung jawab ketersediaan layanan dan dukungan, standar operasi dan prosedur, dan pemenuhan SLA oleh kelompok kerjanya masing-masing.
- Kelompok kerja hubungan pelanggan menyelenggarakan fungsi *Service Desk* karena posisi mereka yang berhadapan langsung dengan pelanggan dalam tugas mereka mengidentifikasi kebutuhan dan mengukur kepuasan terhadap layanan. Mereka yang berperan dalam memotivasi para pengguna layanan agar dapat turut serta dalam mengawasi dan menangani hambatan ketersediaan layanan.
- Kelompok kerja pengiriman layanan bertanggung jawab atas ketersediaan layanan yang dijalankan USI atau yang diminta oleh pelanggan dan bisnis.
- Kelompok kerja multimedia melaksanakan fungsi pengolahan data untuk memenuhi kebutuhan informasi yang diminta pelanggan dan disampaikan oleh kelompok kerja pengiriman layanan.
- Kelompok kerja operasi jaringan bertanggung jawab atas ketersediaan telekomunikasi dan server yang digunakan untuk pencarian dan pengiriman informasi serta penyimpanan data. Merupakan *Network Operations Support*.
- Kelompok kerja workshop memberi bertanggung jawab atas ketersediaan perangkat TIK atau media informasi elektronik. Merupakan *Desktop Support* dan mediator komunikasi antara pelanggan dengan *3rd Party Support*..
- Kelompok kerja pengembangan aplikasi bertanggung jawab atas ketersediaan system informasi. Merupakan *Application Support.*

Pengadaan Perangkat Bantu

Dalam konteks pengendalian keamanan dan ketersediaan layanan, digunakan sejumlah perangkat bantu di antaranya :

- SysAid yakni perangkat lunak berbasis web yang mengotomatisasi proses untuk *Helpdesk*, konfigurasi perangkat keras, pengawasan asset, lisensi perangkat lunak, pekerjaan, proyek, dan lain sebagainya. Perangkat otomatisasi ini memusatkan data pengguna, sejarah permintaan layanan, inventori perangkat lunak dan keras ke dalam antar muka web tunggal yang mudah diakses dan akrab pengguna.
- Symantec Antivirus Server yang digunakan untuk mengelola Anti Virus secara terpusat.
- Network Monitoring yang digunakan untuk memantau ketersediaan perangkat jaringan.

Studi Kasus : Pengendalian Keamanan Perangkat Jaringan



Gambar 9. Impelementasi model dalam pengendalian keamanan perangkat jaringan

Dalam pengendalian keamanan perangkat jaringan, kelompok kerja *Network Operation Support* (NOS) mengawasi ketersediaan perangkat jaringan melalui perangkat pengawasan jaringan seperti CCTV dan *Network Monitoring*. Perangkat pengawas jaringan *Network Monitoring* bekerja pada prinsipnya dengan cara mengirimkan paket data (*Ping*) ke satu persatu perangkat jaringan untuk mendapatkan balasan pengiriman (*Reply*). Setiap balasan pengiriman mengindikasikan ketersediaan perangkat jaringan yang kemudian dipetakan (*Mapping*) oleh perangkat dan dilaporkan kepada NOS.

Pengenalan (*Know*) NOS terhadap ketersediaan perangkat jaringan selain dari perangkat pengawasan jaringan juga dari pelanggan atau dari *Service Desk* melalui registrasi masalah dalam SysAid. Permintaan perbaikan layanan ini mempertegas status ketidaktersediaan perangkat jaringan yang dipetakan oleh perangkat pengawasan jaringan. Hanya saja perangkat pengawas tersebut membantu NOS mengetahui ketidaktersediaan perangkat jaringan tanpa konfirmasi atau komplain dari pelanggan. Dengan demikian, keberadaanya mengesankan penyedia layanan bersikap proaktif, menangani masalah tanpa menunggu laporan dari pelanggan..

Setelah itu, langkah yang harus dilakukan oleh *Technical Support* adalah memahami siapa yang harus menangani hambatan ketersediaan layanan yang

disebabkan karena gangguan pada perangkat jaringan dan bagaimana menanganinya (*How*). Penanganannya dilakukan sesuai dengan SOP dan dilaksanakan oleh pengampu tugas sesuai deskripsi kerja yang ditetapkan kepala USI.

Dalam proses pemeliharaan perangkat jaringan (*Actuating*), diperhatikan oleh pengampu layanan agar dilaksanakan dengan memenuhi SLA agar kepercayaan dan kepuasan pelanggan tetap terjaga.

VI. PENUTUP

Sebagaimana isyarat dari penelitian Robles, Park, dan Kim di mana pemusatan pengendalian keamanan tidak menghilangkan peran pelanggan atau pengguna dalam mengawasi dan melaporkan hambatan ketersediaan layanan [11], model system pengendalian keamanan kolaboratif tetap menjaga peran pengguna dalam penanganan keamanan yang menggangu kepentingannya terhadap layanan. Dengan pendekatan *actor-network theory* [20] dan *distributed cognition* [21], semua entitas kunci tidak dibedakan antara manusia dan bukan manusia, sehingga perangkat yang menjadi fasilitas komunikasi dan alat pengawas ditetapkan sebagai actor atau entitas kunci yang akan berkurang nilai kolaborasinya dengan ketiadaaanya.

Model ini merupakan gambaran tentang bagaimana penerapan pengendalian keamanan dilaksanakan dengan menempatkan pendekatan sentralistik dan desentralistik secara proporsional. Model kolaboratif merupakan rangkaian proses yang mengatur interaksi partisipan yang bekerja sama mencapai tujuan bersama yakni terpenuhi SLA yang dapat menjaga kepercayaan terhadap layanan SI dan kepuasan penggunanya. Pengaturan tersebut diperlukan untuk memastikan setiap partisipan bertindak sesuai dengan perannya masing-masing dan tidak dibebani atau tidak membebani diri dengan aktivitas diluar fungsi dan tanggung jawabnya. Pemetaan model kolaborasi ke dalam kerangka kerja ITIL mensyaratkan penyesuaian organisasi dalam pelaksanaannya sehingga sesuai dengan komponen ITIL.

Dengan ketersediaan rencana pengembangan, sumber daya manusia, pengarahan, komunikasi, dan kepemimpinan yang kuat dari eksekutif, model kolaborasi untuk pengendalian keamanan dapat dilaksanakan.

H. DAFTAR PUSTAKA

[1] Peterson, R.R. (2000). Emerging capabilities for IT Governance: Exploring stakeholder perspective in Financial Service. Conference Proceedings European Conference on Information System 2000, Viena, Austria.

[2] Sambamurthy, V., & Zmud, R. W. (2000). Reserach commentary. The organizing logic for an enterprise's IT activities in the digital age: A prognosis of practice and a call for research. Information System Research, 11(2), 105-114.

[3] Vitale, M. (2001). The dot.com legacy: Governing IT on internet time. Working Paper. Information System Research Center, University of Houston, Houston, Texas, USA.

[4] Whetherbe, J. (2001). Achiefing the high-performance, information-based networked organization. Woring Paper, Information Research Center, University of Houston, Houston, Texas, USA.
[5] Brown, C.V., & Magil, S.L. (1998). Reconceptualizing the contex-design issue for information system function. Organization Science, 9(2), 176-194
[6] King, J.L. (1983). Centralized versus decentralized computing: Organizational considerations and management option. Computing Survey, 15(4), 319-349.
[7] Rockart, J.F., Earl, M., & Ross, J.W. (1996). Eight imperative for new IT organization. Sloan Management Review, 38(1), 32-42.
[8] Mintzberg, H. (1979). The structuring of organizations. Englewood Cliffs: Prentice Hall.
[9] Simon, H.A., & Barnard, C.I. (1961). Administrative Behavior: A study of decision making processes in administrative organization. New York: The Macmillan Company.
[10] Weil, P., & Broadbent, M. (1998). Laveraging the new infrastructure: How market leaders capitalize on information technology. Boston, MA: Harvard Business School Press.
[11] Robles, R. J., Park, J, Kim, T. 2008. Information Security Control Centralization and IT Governance for Enterprise. International Journal of Multimedia and Ubiquitous Engineering. Vol. 3, No. 3.
[12] Peterson, R. R. (2001) Information Governance: An empirical investigation into differentiation and integration stratgic decision-making for IT, The Netherlands: Tilburg University
[13] Henderson, J.C. (1990). Pluging into strategic partnetships: The critical IS connection. Sloan Management Review, 31(3), 7-18.
[14] Webb, P., Pollard, C., and Ridley, G. (2006) "Attempting to define IT Governance: Wisdom or Folly" Proceedings of the 39th Hawaii International Conference on system Sciences,
[15] IT Governance Institute (ITGI), COBIT, 4th Edition, December 2005. Available online at http://www.isaca.org
[16] Weill, P., and Ross, J. W., (2004). IT governance – How top performers manage IT decision rights for superior results. Harvard Business School Press
[17] Office of Government Commerce (OGC). (2002), IT Infrastructure Library Service Delivery. The Stationery Office
[18] Spence, M. U. (2006). "Graphic Design: Collaboration Process = Understand Self and Other" (Lecture) Art 325: Collaborative Process. Fairbanks Hall, Oregon State University, Corvallis, Oregon.
[19] Kaptelinin, V., Nardi B. A. 2006. Acting with Technology: Activity Theory and Interaction Design. The MIT Press, Cambridge, Massachusetts, London, England.
[20] Callon, M., J. Law, and A. Rip. (1986). Mapping the Dynamics of Science and Technology: Sociology of Science in the Real World. London: Palgrave Macmillan.
[21] Hutchins, E. (1995). Cognition in the Wild. Cambridge, Mass.: MIT Press.